**UNITED STATES DISTRICT COURT**
**EASTERN DISTRICT OF PENNSYLVANIA**

| | |
|---|---|
| ANDREW RECCHILONGO, individually and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>CONNEXIN SOFTWARE, INC., d/b/a OFFICE PRACTICUM.<br><br>Defendant. | Case No. 2:23-cv-00068<br><br>**CLASS ACTION COMPLAINT**<br><br>**JURY TRIAL DEMANDED** |

Plaintiff Andrew Recchilongo ("Plaintiff"), individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to themselves and on information and belief as to all other matters, by and through undersigned counsel, bring this Class Action Complaint against Defendant Connexin Software, Inc. d/b/a Office Practicum ("Connexin" or "Defendant").

## NATURE OF THE ACTION

1. Plaintiff brings this class action on behalf of himself and all other individuals ("Class Members") who had their sensitive personal information ("PII") and protected health information ("PHI")—as defined by Health Insurance Portability and Accountability Act ("HIPPA")— disclosed to unauthorized third parties that accessed and removed the PII and PHI from Connexin's system in August 2022 (the "Data Breach"). The compromised PII and PHI includes the following: (1) patient demographic information (such as patient name, guarantor name, parent/guardian name, address, email address, and date of birth); (2) Social Security Numbers ("SSNs"), (3) health insurance information (payer name, payer contract dates, policy information including type and deductible amount and subscriber number); (4) medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Record Numbers); (5) billing

and/or claims information (invoices, submitted claims and appeals, and patient account identifiers used by your provider); and (6) information of a parent, guardian, or guarantor.

2. Connexin Software Inc. is a company that offers pediatric-specific health IT solutions to nearly 120 pediatric medical practices in over 40 states[1] servicing 16 million patients[2] and operates under the name Office Practicum. In November 2022, Connexin notified 2.2 million individuals that it suffered the Data Breach and informed them that their PII and PHI was compromised thereby (the "Notice").

3. According to the Notice—posted on Office Practicum's website[3]—Connexin first detected the Data Breach on August 26, 2022, when it detected a data anomaly on its internal network. Connexin's notice states that it immediately launched an investigation and engaged third-party forensic experts to determine the nature and scope of the incident, which on September 13, 2022, revealed that an unauthorized party was able to gain access to an internal computer network, access an offline set of patient data used for data conversion and troubleshooting, and that the data set was removed by the unauthorized party. Thus, the Data Breach resulted from Connexin's failure to adequately protect and safeguard that offline set of patient data.

4. Thus, Connexin only began informing customers and patients of its Data Breach nearly three months after it experienced the first indication of its occurrence and more than two months after it learned of the unauthorized user access. During that time, however, Connexin notified at least 8 state Attorney Generals of the Data Breach.[4]

5. Connexin's Notice lists 119 separate pediatric practices whose patients' PII and PHI was, or may have been, compromised in the Data Breach.

---

[1] https://www.businesswire.com/news/home/20111116006829/en/Connexin-Software-Inc.-Receives-Strategic-Investment-from-Bluff-Point-Associates-Deal-Will-Accelerate-Growth-and-Leadership-Position-of-Pediatric-EHR-Software-Provider

[2] https://www.officepracticum.com/

[3] https://www.officepracticum.com/substitute-notice/

[4] *Id.*

6. Connexin owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. Connexin breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its patients' PII/PHI from unauthorized access and disclosure.

7. As a result of Connexin's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of himself and all similarly situated individuals whose PII/PHI was exposed as a result of the Data Breach, which Connexin learned of on or about August 26, 2022 but did not publicly disclose until November 2022.

8. Plaintiff, on behalf of himself and all other Class members, asserts claims for negligence, negligence per se, and unjust enrichment, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

## PARTIES

9. Plaintiff is a citizen of the state of Pennsylvania and resides in Drexel Hill, Pennsylvania. Believing his former pediatric healthcare provider would implement and maintain reasonable security and practices to protect his PII and PHI, Plaintiff provided this information to his provider, which utilized Connexin's Office Practicum software. On or about December 2022, Connexin sent Plaintiff, and Plaintiff received, a letter confirming that his PII and PHI was impacted by the Data Breach. In the letter, Connexin identified that the nature of the information involved includes:

(a) patient demographic information (such as patient name, guarantor name, parent/guardian name, address, email address, and date of birth);

(b) Social Security Numbers ("SSNs"),

(c) health insurance information (payer name, payer contract dates, policy information including type and deductible amount and subscriber number);

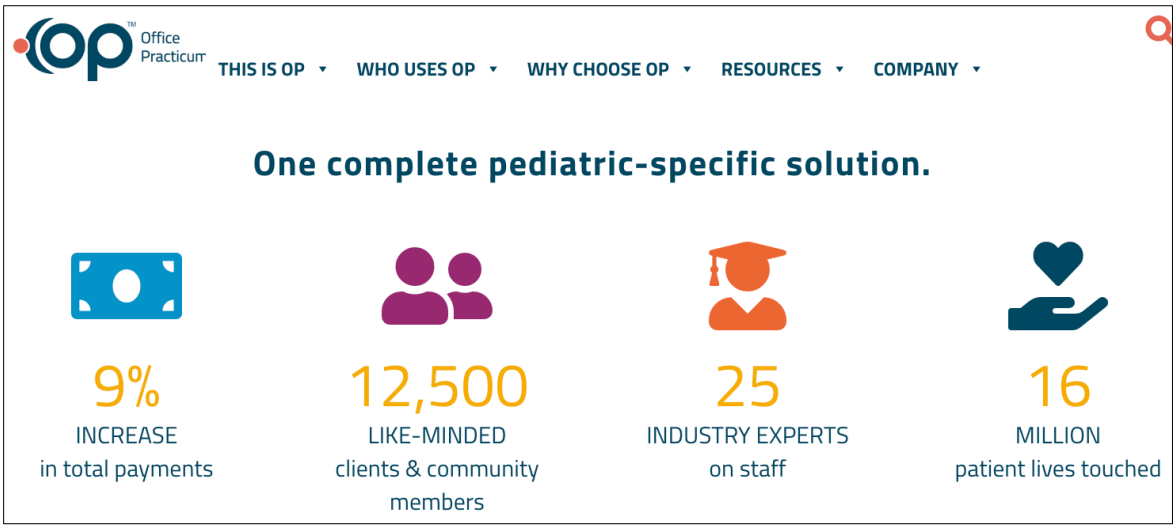
(d) medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Record Numbers);

(e) billing and/or claims information (invoices, submitted claims and appeals, and patient account identifiers used by your provider); and

(f) information of patients' parents, guardians, or guarantors.

Plaintiff has spent approximately an hour monitoring his accounts for fraudulent activity.

10. Defendant Connexin Software, Inc. is incorporated in Maryland and maintains its principal place of business at 602 W. Office Center Drive, Suite 350, Fort Washington, PA 19034.[5] Connexin describes itself as the leading provider of electronic medical records and practice management systems for use in pediatric clinical settings, and that its Office Practicum product has provided innovative solutions to hundreds of medical practices in over 40 states and throughout the Caribbean, ranging from solo providers to hospital-based clinics.[6] Connexin's website states that it has provided services to 16 million patients:




[5] https://egov.maryland.gov/BusinessExpress/EntitySearch/Business

[6]https://www.businesswire.com/news/home/20111116006829/en/Connexin-Software-Inc.-Receives-Strategic-Investment-from-Bluff-Point-Associates-Deal-Will-Accelerate-Growth-and-Leadership-Position-of-Pediatric-EHR-Software-Provider

## JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(a) and (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000.00) and is a class action in which one or more Class Members are citizens of states different from Defendant.

12. The Court has personal jurisdiction over Defendant because it maintains its principal place of business in Pennsylvania, conducts significant business in Pennsylvania, and/or otherwise has sufficient minimum contacts with and intentionally avails itself of the markets in Pennsylvania.

13. Venue properly lies in this district because, *inter alia,* Defendant maintains its principal place of business in this district; transacts substantial business, has agents, and is otherwise located in this district; and/or a substantial part of the conduct giving rise to Plaintiff's claims occurred in this judicial district.

## FACTUAL ALLEGATIONS

### A. Overview of Defendant

14. Defendant is a provider of electronic medical records and practice management software, billing services, and business analytic tools to pediatric physician practice groups."[7]

15. Defendant touts itself as the leading provider of electronic medical records and practice management systems for use in pediatric clinical settings.[8] "Since 1995, its Office Practicum product has provided innovative solutions to hundreds of medical practices in over 40 states and throughout the Caribbean, ranging from solo providers to hospital-based clinics."[9]

---

[7] https://www.officepracticum.com/substitute-notice/

[8] https://www.businesswire.com/news/home/20111116006829/en/Connexin-Software-Inc.-Receives-Strategic-Investment-from-Bluff-Point-Associates-Deal-Will-Accelerate-Growth-and-Leadership-Position-of-Pediatric-EHR-Software-Provider

[9] *Id*.

16. In the regular course of its business, Defendant collects and maintains the PII/PHI of its customers' (i.e., pediatric healthcare providers) patients, former patients, and its patients parents, guardians, or guarantors.[10]

17. That information includes: (1) patient demographic information (such as patient name, guarantor name, parent/guardian name, address, email address, and date of birth); (2) Social Security Numbers ("SSNs"), (3) health insurance information (payer name, payer contract dates, policy information including type and deductible amount and subscriber number); (4) medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Record Numbers); (5) billing and/or claims information (invoices, submitted claims and appeals, and patient account identifiers used by your provider); and (6) information of a parent, guardian, or guarantor. Defendant stores this information digitally.

18. Plaintiff and Class members are, or were, patients of pediatric healthcare providers—or their parents, guardians, or guarantors—that used Defendant's Office Practicum services, and thereby entrusted Defendant with their PII/PHI.

**B. The Data Breach**

19. On August 26, 2022, Defendant detected a data anomaly on its internal network.[11]

20. A subsequent investigation revealed on September 13, 2022 that an unauthorized party was able to gain access to an internal computer network, access an offline set of patient data used for data conversion and troubleshooting, and that the data set was removed by the unauthorized party.[12]

21. Thus, the Data Breach resulted from Connexin's failure to adequately protect and

[10] https://www.officepracticum.com/substitute-notice/
[11] *Id.*
[12] *Id.*

safeguard that offline set of patient data. Defendant has not revealed how long cybercriminals may have had access to its network or patients' PII/PHI.

22. Defendant began to notify patients about the Data Breach on or about mid-to-late November 2022.[13] The Notice that Defendant sent to Plaintiff and the Class state that the information that was accessed included:

(a) patient demographic information (such as patient name, guarantor name, parent/guardian name, address, email address, and date of birth);

(b) Social Security Numbers ("SSNs"),

(c) health insurance information (payer name, payer contract dates, policy information including type and deductible amount and subscriber number);

(d) medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Record Numbers);

(e) billing and/or claims information (invoices, submitted claims and appeals, and patient account identifiers used by your provider); and

(f) information of patients' parents, guardians, or guarantors.[14]

**C. Defendant Knew that Criminals Target PII/PHI**

23. At all relevant times, Defendant knew, or should have known, its customers' patients', Plaintiff's, and all other Class members' PII/PHI was a target for malicious actors. Despite such knowledge, Defendant failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII/PHI from cyber-attacks that Defendant should have anticipated and guarded against.

24. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2021 report, the healthcare compliance company Protenus found that there were

[13] *Id.*
[14] *Id.*

758 medical data breaches in 2020 with over 40 million patient records exposed.[15] This is an increase from the 572 medical data breaches that Protenus compiled in 2019.[16]

25. PII/PHI is a valuable property right.[17] The value of PII/PHI as a commodity is measurable.[18] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[19] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[20] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

26. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, SSNs, PII/PHI, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

---

[15] Protenus, *2021 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/resources/2021-breach-barometer (last accessed Nov. 15, 2021).
[16] Protenus, *2020 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/resources/2020-breach-barometer (last accessed Nov. 15, 2021).
[17] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data
[18] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.
[19] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.
[20] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

27. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[21] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[22] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[23]

28. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[24] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[25]

29. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[26] Quoting Carbon Black's Chief Cybersecurity

---

[21] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon ("*What Happens to Stolen Healthcare Data* Article") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[22] *Id.*

[23] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims.

[24] SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAGAZINE (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

[25] Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

[26] *What Happens to Stolen Healthcare Data*, *supra* at n.10.

Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[27]

30. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[28]

31. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

**D. Theft of PII/PHI Has Grave and Lasting Consequences for Victims**

32. Theft of PII/PHI is serious. The FTC warns consumers that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[29]

33. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[30] According to Experian, one of the

---

[27] *Id.*

[28] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

[29] *See* Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Nov. 15, 2021).

[30] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction

largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[31]

34. With access to an individual's PII/PHI, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[32]

35. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[33]

---

with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

[31] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (Sept. 1, 2017), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[32] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Nov. 15, 2021).

[33] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE

36. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

37. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[34]

38. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[35] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[36] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[37] The FTC also warns, "If the thief's health information is mixed with yours, your

---

CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed Nov. 15, 2021).

[34] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

[35] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), https://www.ftc.gov/system/files/documents/public_comments/2018/01/00037-142815.pdf

[36] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk*…, *supra* at n.14.

[37] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, Federal Trade Commission Consumer Information, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Nov. 15, 2021).

treatment, insurance and payment records, and credit report may be affected."[38]

39. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services not sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[39]

40. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used and it takes some individuals up to three years to learn that information.[40]

---

[38] *Id*.
[39] *See* Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, *supra* at 24.
[40] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics,

41. It is within this context that Plaintiff and all other Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

**E. Damages Sustained by Plaintiff and the Other Class Members**

42. Plaintiff and all other Class members have suffered injury and damages, including, but not limited to: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face.

## CLASS ALLEGATIONS

43. Plaintiff brings this action on behalf of himself and the following class:

> All residents of the United States who were notified by Defendant that their PHI and PII may have been compromised as a result of the Data Breach.

44. Excluded from the Class are: (1) the Judges presiding over the Action, Class Counsel, and members of their families; (2) the Defendant, its subsidiaries, parent companies, successors, predecessors, and any entity in which Defendant or their parents, have a controlling interest, and their current or former officers and directors; (3) Persons who properly opt out; and (4) the successors or assigns of any such excluded Persons.

---

Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

45. **Numerosity**: Members of the class are so numerous that their individual joinder is impracticable, as the proposed class includes 2.2 million members who are geographically dispersed.

46. **Typicality**: Plaintiff's claims are typical of class members' claims. Plaintiff and all class members were injured through Defendant's uniform misconduct, and Plaintiff's claims are identical to the claims of the class members they seek to represent. Accordingly, Plaintiff's claims are typical of class members' claims.

47. **Adequacy**: Plaintiff's interests are aligned with the class they seek to represent and Plaintiff has retained counsel with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Plaintiff and his counsel intend to prosecute this action vigorously. The class's interests are well-represented by Plaintiff and undersigned counsel.

48. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiff's and other class member's claims. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for class members individually to effectively redress Defendants' wrongdoing. Even if class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

49. **Commonality and Predominance:** The following questions common to all class members predominate over any potential questions affecting individual class members:

a. Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class Members' PII/PHI from unauthorized access and disclosure;

b. Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiff's and Class Members' PII/PHI;

c. Whether an implied contract existed between Class members and Defendant providing that Defendant would implement and maintain reasonable security measures to protect and secure Class members' PII/PHI from unauthorized access and disclosure;

d. Whether Defendant breached its duties to protect Plaintiff's and Class members' PII/PHI; and

e. Whether Plaintiff and all other members of the Class are entitled to damages and the measure of such damages and relief.

50. Given that Defendants engaged in a common course of conduct as to Plaintiff and the class, similar or identical injuries and common law and statutory violations are involved, and common questions outweigh any potential individual questions.

## CAUSES OF ACTION

## COUNT I

## NEGLIGENCE

51. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

52. Defendant owed a duty to Plaintiff and all other Class members to exercise reasonable care in safeguarding and protecting their PII/PHI in its possession, custody, or control.

53. Defendant knew the risks of collecting and storing Plaintiff's and all other Class members' PII/PHI and the importance of maintaining secure systems. Defendant knew of the many data breaches that targeted healthcare providers in recent years.

54. Given the nature of Defendant's business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, Defendant should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

55. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiff's and Class members' PII/PHI.

56. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

57. But for Defendant's negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised.

58. As a result of Defendant's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national

and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

## COUNT II

## NEGLIGENCE PER SE

59. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

60. Defendant's duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

61. Defendant's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as Defendant, of failing to employ reasonable measures to protect and secure PII/PHI.

62. Defendant violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other Class members' PII/PHI and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

63. Defendant's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

64. Plaintiff and Class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

65. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

66. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

67. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Defendant's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

## COUNT III

## UNJUST ENRICHMENT

68. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

69. This claim is pleaded in the alternative to the breach of implied contract claim.

70. Plaintiff and Class Members have both a legal and equitable interest in their PHI and PII that was collected by, stored by, and maintained by Defendant—thus conferring a benefit upon Defendant—that was ultimately compromised by the Data Breach.

71. Defendant accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Defendant also benefitted from the receipt of Plaintiff's and Class members' PHI.

72. As a result of Defendant's failure to safeguard and protect Plaintiff's PII and PHI, conduct, Plaintiff and Class members suffered actual damages.

73. Defendant should not be permitted to retain the benefit belonging to Plaintiff and Class members because Defendant failed to adequately implement the data privacy and security procedures for itself that were mandated by federal, state, and local laws and industry standards.

74. Defendant should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

## COUNT IV

## DECLARATORY RELIEF
## (28 U.S.C. § 2201)

75. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

76. An actual controversy has arisen and exists between Plaintiff and members of the Class, on the one hand, and Defendant, on the other hand, concerning the Data Breach and

Defendants' failure to protect Plaintiff's and class members' PHI and PII, including with respect to the issue of whether Defendant took adequate measures to protect that information. Plaintiff and class members are entitled to judicial determination as to whether Defendant has performed and are adhering to all data privacy obligations as required by law or otherwise to protect Plaintiff's and class members PHI and PII from unauthorized access, disclosure, and use.

77. A judicial determination of the rights and responsibilities of the parties regarding Defendant's privacy policies and whether they failed to adequately protect PHI and PII is necessary and appropriate to determine with certainty the rights of Plaintiff and the class members, and so that there is clarity between the parties as to Defendant's data security obligations with respect to PHI and PII going forward, in view of the ongoing relationships between the parties.

## PRAYER FOR RELIEF

Plaintiff, individually and on behalf of the class members, by and through undersigned counsel, respectfully request that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiff as class representative and undersigned counsel as class counsel;

B. Award Plaintiff and class members actual and statutory damages, punitive damages, and monetary damages to the maximum extent allowable;

C. Award declaratory and injunctive relief as permitted by law or equity to assure that class members have an effective remedy, including enjoining Defendant from continuing the unlawful practices as set forth above;

D. Award Plaintiff and class members pre-judgment and post-judgment interest to the maximum extent allowable;

E. Award Plaintiff and class members reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Award Plaintiff and Class Members such other favorable relief as allowable under law or at equity.

**JURY TRIAL DEMANDED**

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: January 6, 2023

Respectfully submitted,

*/s/ Andrew W. Ferich*

Andrew W. Ferich (SBN 313696)
**AHDOOT & WOLFSON, PC**
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: 310.474.9111
Facsimile: 310.474.8585
*aferich@ahdootwolfson.com*

Tina Wolfson (*pro hac vice* to be filed)
**AHDOOT & WOLFSON, PC**
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505-4521
Telephone: 310.474.9111
Facsimile: 310.474.8585
*twolfson@ahdootwolfson.com*

Joseph B. Kenney (SBN 316557)
Mark B. DeSanto (SBN 320310)
**SAUDER SCHELKOPF LLC**
1109 Lancaster Avenue
Berwyn, PA 19312
Telephone: (888) 711-9975
Facsimile: (610) 421-1326
*jbk@sstriallawyers.com*
*mbd@sstriallawyers.com*

*Attorneys for Plaintiff and the Proposed Class*